

# Weekly Report

May 12, 2019

## 1 Work

1. 本周在进行unpair setting下的图片增强，本周测试了(1) 无style code (2) style code concat 等情况，效果均不理想。
2. Adversarial Attack使用字典直接学习对抗样本，程序没问题，但是结果是没有进攻成功，接下来准备换一个优化方式。
3. 工作时长：工作日每天10个小时，周末共12个小时，共62个小时。

### 1.1 工作进度

Table 1: 工作进度

项目	进度	截止时间
DRGraph	正在修改代码	
unpair 低光照图片增强	目前初步的实验效果不佳	
NIPS	基于字典学习Adversarial Attack	2019.5.23

## 2 Paper Reading

### 2.1 Learning to Anonymize Faces for Privacy Preserving Action Detection

对抗样本的一个应用，在保持视频可以被检测出行为的情况下，保护人脸个人信息。

### 2.2 Unsupervised Image Super-Resolution using Cycle-in-Cycle Generative Adversarial Networks

本文使用两个Unpaired CycleGAN完成了低分辨率图片->去噪低分辨率图片->高分辨率图片的变化。

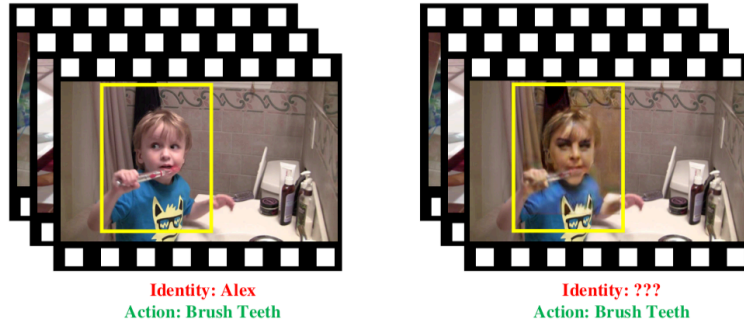


Figure 1: #1

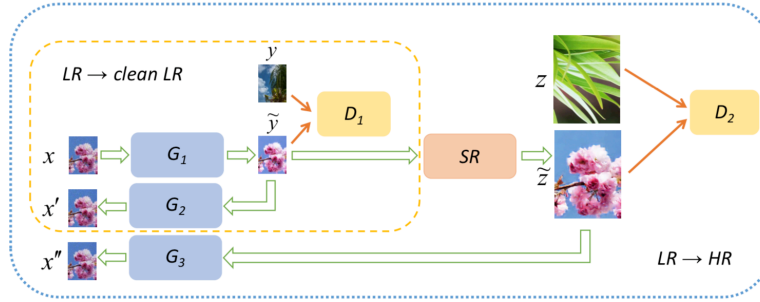


Figure 2: #2

### 2.3 Generating Adversarial Examples with Adversarial Networks

本文使用了GAN来生成对抗样本。相比于以前的基于梯度的优化方法，本文的方法支持快速生成对抗样本，可以进攻黑盒样本，并且生成的对抗样本非常接近于真实图片（无法分辨真假）。

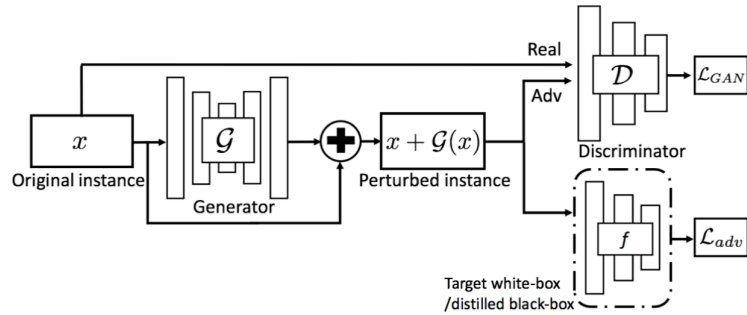


Figure 3: #3

### 2.4 Spatial Transformer Networks

当前的训练数据都是经过预处理，比如图片的目标基本上处于正中间。当分类目标存在旋转缩放扭曲等现象时，分类器的效果就会受到影响。因此，本文提出使用神经网络

络来自适应地学习这些空间变化，可以提升网络对输入图片的鲁棒性。